Webinar Questions

1. Do you have a version of this that would be appropriate for C level / Board presentation? (10-15 minutes, in a form that speaks to the high-level need of the board but still presents a sense of urgency to motivate them to move on this topic)

MIKE SEMEL: We do presentations for owners of small practices to executives and boards of larger organizations. Each presentation is focused on the needs of the organization. Our general message about technology can be found in the slides, which you can shorten for your needs.

The cost of a health care data breach- based on real research- is $ 398 per record, including the costs of dealing with the breach and the lost business afterwards. A data breach could bankrupt and organization and when it hits the news the media won't be calling the IT guys, they will be calling the CEO. Remind the C-levels about the headline from Forbes Magazine- *Target CEO Gregg Steinhafel Resigns In Data Breach Fallout.*

Besides the fact that this is a top-management issue, the executives and the boards need to understand that:

- Risks of data breaches and compliance violations continually increase
- The Federal Trade Commission is now enforcing data breaches and caused a lab to close
- 1,200 HIPAA audits will be taking place soon and the time to respond will be very short
- Most IT departments and solution providers are expert on keeping networks running, not security
- Cloud-based services create unique risks that must be managed
- Our experience doing audits every day show that the technology in healthcare organizations is not secure or compliant, in spite of what we are told
- Technology is complex and needs oversight, similar to their accounting systems and processes, that receive regular independent audits

This is what the FBI warned health care organizations about the security of their data:
The biggest vulnerability was the perception of IT healthcare professionals' beliefs that their current perimeter defenses and compliance strategies were working when clearly the data states otherwise.

Can all that fit into 15 minutes?

Is there anything that you need in addition to paperwork to prove encryption on a laptop or thumb drive?

MIKE SEMEL: The challenge of proving encryption is that you will need to prove it after a device was lost or stolen. Your question depends on what you define as paperwork. If paperwork is a receipt showing the purchase of encryption tools that would not prove that they were properly installed and are working. There are systems that monitor the status of laptops to ensure that encryption is properly installed and working. There are security tools that can force thumb drives to be encrypted before data can be transferred. Each of these tools has reporting capabilities that could show that a device was encrypted before it was lost or stolen.

Many of the practices I deal with have put residential quality routers/firewalls in place and not commercial grade security units.
MIKE SEMEL: A residential-quality (or consumer-grade) router/firewall does not have the Intrusion Prevention capabilities built into a business-grade firewall.

More important, a business-grade firewall must be purchased with the right security features, configured properly, have a current security subscription, and be monitored to ensure its security is working properly. In 2014, a small non-profit paid $ 150,000 for "by failing to ensure that firewalls were in place with threat identification monitoring of inbound and outbound traffic and that information technology resources were both supported and regularly updated with available patches."

These features are not available on residential quality devices.

What is your view on medical practice that are not concerned with compliance because they say their EMR is in the cloud?
MIKE SEMEL: Any practice that thinks HIPAA doesn't apply to them because their EMR is in the cloud does not understand HIPAA and risks data breaches and compliance violations. Moving their EMR system to the cloud reduces some of the technical requirements, but adds other risks for the practice. HIPAA consists of the Privacy, Security, Data Breach, and Omnibus Final Rules. The Security Rule that focuses on the security of health data is mostly made up of Administrative Controls- the policies, procedures and training to secure data.

What would you recommend for a cost effective encryption solution (1) for small office providers and (2) for critical access hospitals?
MIKE SEMEL: Encryption doesn't have to be expensive. New Apple and business-class Windows-based computers have encryption capabilities built in, so encryption is already part of your purchase. Some encryption tools that can be added on to Windows 7, and other systems that do not include native encryption, can be purchased as a service for a low monthly cost per user. Talk to your IT vendor about Encryption-as-a-Service.

Would you suggest having backup CDs/DVDs that contain Ultrasounds, x-rays, etc encrypted when stored at an offsite Medical Record storage facility?
MIKE SEMEL: Yes, because loss or theft from the storage facility is possible. More likely, loss or theft on the way to, or back from, the storage facility is very likely. If the unencrypted media is lost then every patient whose data was breached will have to be notified, the OCR and possibly your state attorney general will need to be informed, you could be fined, and you could lose patients. Remember that the 2015 cost of a data breach is $ 398 per record. If encrypted data is lost you do not have to report it.

Anytime you have a HIPAA question feel free to e-mail me at mike@semelconsulting.com .